AXIS Camera Station Pro

Przewodnik zabezpieczania systemów

Wprowadzenie

Uniwersalna, w pełni niezawodna funkcja, dzięki której każdy system bezpieczeństwa i każdy obiekt fizyczny będą w 100% odporne na cyberataki. Jakkolwiek atrakcyjnie brzmią te słowa, taka funkcja nie istnieje — ani raczej nie powstanie w najbliższym czasie. Dlatego zamiast jej szukać, należy ocenić ryzyko stwarzane przez zagrożenia i luki w zabezpieczeniach charakterystyczne dla danej organizacji, a gdy ryzyko to okaże się nie do zaakceptowania — wdrożyć mechanizmy kontrolne w celu jego ograniczenia. Dobrze zdefiniowane zasady i procedury zapewniają spójne komunikowanie oraz stosowanie tych mechanizmów w całej organizacji i stanowią podstawę dojrzałego programu cyberbezpieczeństwa.

W prowadzonych działaniach najlepiej kierować się znormalizowanymi ramami zarządzania zagrożeniami bezpieczeństwa w środowiskach IT, takimi jak ISO 27001, NIST CSF itp. Chociaż w mniejszych organizacjach to zadanie może wywoływać zniechęcenie, zdefiniowanie podstawowego zestawu zasad bezpieczeństwa informacji i towarzyszących im procesów jest znacznie lepsze niż całkowita bierność w tym zakresie. Jeśli dana organizacja dopiero stawia pierwsze kroki na drodze do dojrzałości cybernetycznej i dysponuje ograniczonymi zasobami, zalecamy zapoznanie się z dokumentem *Center for Internet Safety (CIS) Critical Security Controls Version 8*. CIS przedstawia listę 18 działań z zakresu kontroli bezpieczeństwa podzielonych na trzy grupy wdrożeniowe, która pomaga organizacjom w opracowaniu i doskonaleniu własnego programu cyberbezpieczeństwa.

W wielu organizacjach dochodzi do naruszenia zabezpieczeń, ponieważ nie zdefiniowały one jasnych zasad, reguł i procedur regulujących korzystanie z systemów i uprawnienia dostępu własnych pracowników. A czy w Twojej organizacji obowiązują zasady i procedury dotyczące zarządzania materiałem wizyjnym? Jeśli nie, najwyższy czas przystąpić do ich sformułowania.

Przeznaczenie

W niniejszym dokumencie przedstawiono szereg przydatnych zasad i procedur cyberbezpieczeństwa, które pomagają w bezpiecznym wdrażaniu i utrzymywaniu systemów wykorzystujących oprogramowanie AXIS Camera Station Pro. Chociaż nie są one bezpośrednim odwzorowaniem określonych ram cyberbezpieczeństwa, autorzy dokumentu oparli się głównie na dokumencie CIS Security Controls v8 ze szczególnym uwzględnieniem następujących mechanizmów kontrolnych:

- *Mechanizm 1: Inwentaryzacja i kontrola aktywów przedsiębiorstwa*
- *Mechanizm 2: Inwentaryzacja i kontrola aktywów oprogramowania*
- *Mechanizm 3: Ochrona danych*
- *Mechanizm 4: Bezpieczna konfiguracja zasobów i oprogramowania przedsiębiorstwa*
- *Mechanizm 5: Zarządzanie kontami*
- *Mechanizm 6: Zarządzanie kontrolą dostępu*
- *Mechanizm 7: Stałe zarządzanie lukami w zabezpieczeniach*
- *Mechanizm 10: Ochrona przed złośliwym oprogramowaniem*

Głównym celem naszych zaleceń jest wsparcie instalatorów, integratorów i użytkowników w ograniczaniu typowych zagrożeń mogących wystąpić podczas wdrażania systemów wykorzystujących oprogramowanie AXIS Camera Station Pro oraz zarządzania nimi.

Wymagania wstępne

Zakłada się, że zalecenia oraz procedury określone i opisane w *przewodniku po zabezpieczeniach systemu AXIS OS* zostały przyswojone i zastosowane. Ponadto niniejszy dokument zawiera odniesienia do kilku typowych ról użytkowników wchodzących w interakcję z systemem wizyjnym. Role te należy zaadaptować do rzeczywistej klasyfikacji użytkowników i ról stosowanej w danej organizacji. W zależności od organizacji jeden użytkownik może mieć wiele ról.

Zdefiniowane role:

- **Instalator systemów**: instaluje, konfiguruje i naprawia systemy oraz podwyższa i obniża poziom ich zaawansowania

Wprowadzenie

- **Administrator sieci**: dba o infrastrukturę sieciową, połączenia węzłów końcowych, serwery i zasoby sieciowe, a także ochronę sieci
- **Administrator systemu wizyjnego**: definiuje system wizyjny i zarządza nim w sposób zabezpieczający jego użytkowanie, wydajność i uprawnienia użytkowników
- **Konserwator systemu wizyjnego**: monitoruje i reguluje elementy oraz rozwiązuje dotyczące ich problemy w imieniu administratora systemu wizyjnego w celu zapewnienia wysokiej wydajności systemu
- **Użytkownicy**: osoby, które za pomocą klienta AXIS Camera Station Pro uzyskują dostęp do przekazywanego na żywo i nagranego materiału wideo oraz zazwyczaj są odpowiedzialne za fizyczną ochronę organizacji.

Zasady bezpieczeństwa systemu

Bezpieczeństwo fizyczne

Zasady ochrony fizycznej

Serwery, urządzenia, sprzęt sieciowy i kable są przedmiotami fizycznymi, które mogą się stać obiektem zakłóceń, sabotażu lub kradzieży. Host, na którym jest uruchomione oprogramowanie serwera AXIS Camera Station Pro, oraz ważne urządzenia sieciowe (routery, przełączniki itp.) powinny być umieszczone w środowisku z dostępem ograniczonym pod względem fizycznym i logicznym. Kamery i inne podłączane urządzenia powinny być montowane w trudno dostępnych miejscach w postaci modeli wandaloodpornych lub wewnątrz obudów wandaloodpornych. Należy zwrócić uwagę na zabezpieczenie kabli w ścianach lub korytkach kablowych, ponieważ zwiększają one ryzyko manipulacji i sabotażu.

Zalecane zasady i procedury
Należy wyznaczyć osobę lub jednostkę organizacyjną odpowiedzialną za wzrokowe kontrolowanie fizycznej ochrony serwerów VMS, sprzętu sieciowego, podłączonych urządzeń i okablowania z określoną częstotliwością. Niezbędne jest prowadzenie dokładnej ewidencji wszystkich serwerów i urządzeń, w tym ich lokalizacji.

Zarządzanie oprogramowaniem

Zasady dotyczące aplikacji innych firm

Ponieważ oprogramowanie AXIS Camera Station Pro jest instalowane w standardowym środowisku Windows, może się pojawić pokusa, by wykorzystać to środowisko do aplikacji niezwiązanych z zarządzaniem materiałem wizyjnym. Jednak instalowanie aplikacji innych firm stwarza możliwość wprowadzenia do środowiska złośliwego oprogramowania, co może doprowadzić do przestojów systemu lub otworzyć tajne drzwi przed hakerami i umożliwić im wejście do sieci organizacji.

Zalecane zasady i procedury
Na sprzęcie hosta nie należy uruchamiać żadnych innych aplikacji poza oprogramowaniem serwera AXIS Camera Station Pro i zaufanymi integracjami innych firm. Jeśli fizyczne elementy sprzętowe mają być wykorzystywane do innych celów, zaleca się używanie wielu instancji serwera wirtualnego i uruchamianie oprogramowania serwera AXIS Camera Station Pro na jednej maszynie wirtualnej, a aplikacji innych firm niezwiązanych z systemem VMS na innej maszynie wirtualnej. Informacje na temat uruchamiania oprogramowania AXIS Camera Station Pro w środowisku wirtualnym można znaleźć *tutaj*.

Zaleca się wdrożenie oprogramowania antywirusowego na wszystkich serwerach i komputerach łączących się z serwerem AXIS Camera Station Pro. Jeśli są wdrożone urządzenia mobilne, ta zasada obejmuje zadbanie o to, aby na urządzeniach były zainstalowane najnowsze systemy operacyjne i poprawki (choć nie bezpośrednio antywirusowe). W przypadku skanowania antywirusowego nie należy skanować katalogów i podkatalogów zawierających bazy danych nagrań. Skanowanie tych katalogów w poszukiwaniu wirusów może wpłynąć na wydajność systemu.

Zarządzanie kontami

Ogólne zasady dotyczące kont

Czasami uprawnienia na poziomie administratora są dla wygody przyznawane zwykłym użytkownikom. W wielu organizacjach nie jest jasne, kto odpowiada za sprawdzanie uprawnień do kont i monitorowanie dostępu pracowników do systemów.

Zalecane zasady i procedury
Zalecamy, aby podczas definiowania kont w systemie organizacje przestrzegały zasady najmniejszych uprawnień. Oznacza to, że uprawnienia dostępu użytkowników są ograniczone tylko do zasobów niezbędnych do wykonywania ich konkretnych zadań służbowych. Zaleca się również okresowe przeprowadzanie audytu uprawnień kont użytkowników systemu w celu ochrony przed zjawiskiem „pełzania uprawnień".

AXIS Camera Station Pro — zasady dotyczące kont administratorów

Częstym błędem podczas wdrażania oprogramowania AXIS Camera Station Pro w środowisku Windows jest zdefiniowanie jednego konta administratora hosta Windows. Z czasem hasło do tego konta może zostać udostępnione w obrębie organizacji, co wiąże się z

ryzykiem uzyskania uprawnień administratora środowiska Windows przez osoby nieupoważnione. Łatwo może to doprowadzić do sytuacji, w której na serwerze zostaną zainstalowane liczne niechciane aplikacje użytkowników lub złośliwe oprogramowanie.

Zalecane zasady i procedury
Komputer z systemem Windows, na którym działa serwer AXIS Camera Station Pro, powinien mieć co najmniej jedno uprzywilejowane konto administratora i jedno uprzywilejowane konto użytkownika. Żadne z tych kont nie powinno być takie samo jak domyślne konto administratora systemu Windows. Domyślne konto administratora należy wyłączyć po utworzeniu uprzywilejowanych kont administratora i użytkownika. Po wdrożeniu hasło do konta administratora powinno być znane wyłącznie **administratorom sieci** i używane wyłącznie przez nich. Uprzywilejowane konto użytkownika powinno być używane przez **administratora systemu wizyjnego** w przypadku, gdy musi on zalogować się do serwera AXIS Camera Station Pro. Należy zauważyć, że nawet jeśli powyższe dwie role pełni ta sama osoba, ze względów kontrolnych i tak zaleca się utrzymywanie oddzielnych kont administratora sieci i administratora systemu wizyjnego. Aby umożliwić obsługę innych zdefiniowanych wcześniej ról, dla każdego **użytkownika**, który będzie się logował do systemu, należy utworzyć kolejne nieuprzywilejowane konto użytkownika.

Jeśli host obsługujący oprogramowanie AXIS Camera Station Pro znajduje się w środowisku domeny Windows Active Directory, można utworzyć konta administratorów i użytkowników w kontekście domeny lub do uwierzytelnienia na hoście AXIS Camera Station Pro może posłużyć istniejące konto domenowe pracownika. To może uprościć zarządzanie kontami, ponieważ nie ma potrzeby tworzenia i utrzymywania dodatkowych kont. Ponadto takie rozwiązanie stwarza możliwość użycia funkcji Zarządzanie zasadami grupy w celu wymuszania złożoności haseł, wdrażania certyfikatów i korzystania z innych funkcji zabezpieczeń dostępnych w środowiskach domenowych.

AXIS Camera Station Pro — zasady dotyczące kont użytkowników

W oprogramowaniu AXIS Camera Station Pro konta użytkowników są przypisane do określonych ról, które z kolei przekładają się na konkretne uprawnienia każdego użytkownika w systemie, takie jak dostępne dla niego widoki i materiał wideo. Jeśli z jednego konta użytkownika korzysta wiele osób, rośnie ryzyko udostępnienia hasła innym osobom w organizacji. Współdzielenie kont powoduje również, że ustalenie, kto uzyskał dostęp do określonej kamery / określonego materiału wideo o określonej porze, jest praktycznie niemożliwe.

Zalecane zasady i procedury

Do uwierzytelniania użytkowników klienta AXIS Camera Station Pro zalecamy korzystanie z protokołu **Kerberos**, patrz .

W miarę możliwości warto korzystać z usługi Microsoft Active Directory w celu łatwego zarządzania użytkownikami i grupami. Warto także dopilnować, aby przed skonfigurowaniem systemu zostały zdefiniowane odpowiednie grupy zabezpieczeń dla wszystkich ról użytkowników.

Active Directory udostępnia również następujące funkcje:

- Zasady haseł wymagające od użytkowników regularnej zmiany hasła
- Ochrona przed atakiem siłowym, dzięki której konto Windows AD jest blokowane po kilku nieudanych próbach uwierzytelnienia zgodnie z określonymi w organizacji zasadami haseł
- Uprawnienia oparte na rolach, umożliwiające stosowanie mechanizmów kontroli dostępu w całej domenie

Jeśli konieczne jest korzystanie z lokalnych kont systemu Windows, zaleca się utworzenie unikatowego konta dla każdego użytkownika systemu i przyznanie mu dostępu tylko do tych elementów systemu, które są mu niezbędne do wykonywania obowiązków. Korzystanie z grup użytkowników może uprościć przydzielanie uprawnień, jeśli jest wielu użytkowników z identycznymi uprawnieniami.

Uwierzytelnianie przy użyciu protokołu Kerberos

AXIS Camera Station Pro korzysta ze zintegrowanego uwierzytelniania systemu Windows na potrzeby uwierzytelniania użytkowników klienta AXIS Camera Station Pro. AXIS Camera Station Pro korzysta z protokołu Microsoft Negotiate (SPNEGO), co oznacza, że preferowanym i domyślnym protokołem uwierzytelniania jest Kerberos. Protokół Negotiate próbuje używać Kerberosa, a w sytuacjach awaryjnych korzysta z NTLM.

Aby korzystać z protokołu Kerberos, należy zarejestrować główne nazwy usług (tzw. SPN) w usłudze Active Directory za pomocą następującego polecenia:

```
setspn -s ACSService/{HOST} {NAZWA_KONTA}
```

HOST – Nazwa hosta serwera, na którym działa serwer AXIS Camera Station Pro.

NAZWA KONTA – Nazwa komputera (konta komputera), na którym działa serwer AXIS Camera Station Pro.

Aby protokół Kerberos działał poprawnie, zalecamy zarejestrowanie zarówno krótkiej nazwy hosta, jak i w pełni kwalifikowanej nazwy domeny (FQDN) docelowego serwera AXIS Camera Station Pro.

Przykład:

```
setspn -s ACSService/CompanyServer CompanyServerAccount setspn -s
ACSService/CompanyServer.domain.local CompanyServerAccount
```

Więcej informacji: *Setspn na stronie microsoft.com.*

Zasady dotyczące kont urządzeń

Konta w urządzeniach Axis to przede wszystkim konta komputerów/klientów. **Użytkownicy** nigdy nie powinni mieć bezpośredniego dostępu do urządzeń. Jedynym klientem, który powinien mieć dostęp do urządzeń podczas normalnej eksploatacji, jest serwer AXIS Camera Station Pro. Powszechnie stosowaną strategią jest ustawienie tego samego hasła we wszystkich urządzeniach. Wprowadza to dodatkowy czynnik ryzyka, ale może również uprościć zarządzanie hasłami, dlatego należy rozważyć stopień własnej tolerancji na ryzyko. Oprogramowanie AXIS Camera Station Pro umożliwia przypisanie każdemu urządzeniu unikatowego hasła za pośrednictwem swojego interfejsu zarządzania.

Częstym błędem jest dodawanie urządzeń do oprogramowania AXIS Camera Station Pro przy użyciu jednego konta współdzielonego przez wiele ról. W pewnym momencie, gdy **konserwator systemu wizyjnego** musi użyć przeglądarki, aby coś zmodyfikować, dochodzi do ujawnienia hasła do konta głównego (root) urządzenia. W ciągu kilku miesięcy większość osób w organizacji pozna hasło do wszystkich urządzeń i uzyska uprawnienia administracyjne w systemie.

Zalecane zasady i procedury
Urządzenie powinno mieć co najmniej dwa konta administracyjne: unikatowe konto utworzone na potrzeby administratorów urządzeń oraz domyślne konto root służące do dodawania urządzeń do serwera AXIS Camera Station Pro. Dostęp tymczasowy, na przykład gdy **konserwator systemu wizyjnego** uzyskuje dostęp do urządzenia za pomocą przeglądarki internetowej, powinien się odbywać przy użyciu kont tymczasowych.

Jako podstawowe narzędzie do zarządzania kontami i hasłami urządzeń powinna być używana aplikacja AXIS Device Manager. Jej wersja jest wbudowana bezpośrednio w oprogramowanie AXIS Camera Station Pro i dostępna na karcie Management (Zarządzanie). Hasło root urządzenia powinno być używane tylko przez aplikację AXIS Device Manager i oprogramowanie AXIS Camera Station Pro oraz znane wyłącznie osobom, które używają aplikacji AXIS Device Manager lub oprogramowania AXIS Camera Station Pro jako narzędzia do zarządzania urządzeniami.

Gdy ktoś z rolą konserwatora musi skorzystać z przeglądarki internetowej, aby uzyskać dostęp do urządzenia lub urządzeń w celu rozwiązania problemu lub przeprowadzenia konserwacji, należy przydzielić konto tymczasowe za pomocą oprogramowania AXIS Camera Station Pro. W tym celu należy wybrać urządzenie lub urządzenia i utworzyć nowe konto, najlepiej z uprawnieniami operatora, z którego będzie mógł korzystać konserwator. Po zakończeniu prac należy usunąć konto tymczasowe.

Konserwacja systemu

AXIS Camera Station Pro Zasady wprowadzania poprawek na hostach Windows

AXIS Camera Station Pro obejmuje serwer i klientów działających w środowisku Windows. Ważne jest aktualizowanie tych systemów, ponieważ daje ono pewność, że systemy obsługujące oprogramowanie AXIS Camera Station Pro nie mają luk w zabezpieczeniach, które można by wykorzystać w celu uzyskania nieautoryzowanego dostępu do systemu zarządzania materiałem wizyjnym.

Zalecane zasady i procedury
W przypadku wszystkich systemów AXIS Camera Station Pro, niezależnie od tego, czy działają na rejestratorach NVR Axis czy na sprzęcie niestandardowym, zaleca się wyłączenie automatycznej aktualizacji. Aktualizacje systemu operacyjnego Windows nie raz powodowały jego niestabilność, dlatego zaleca się, aby dostępne aktualizacje były testowane na wybranych komputerach w celu zweryfikowania stabilności, zanim zostaną one przekazane do wszystkich systemów obsługujących oprogramowanie AXIS Camera Station Pro. Należy jednak zadbać o równowagę między bezpieczeństwem a stabilnością, ponieważ zbyt długie pozostawianie systemu Windows bez poprawek może stanowić zagrożenie dla całego środowiska. Zależnie od stopnia narażenia systemu klienta na zagrożenia zewnętrzne w zasadach wprowadzania poprawek należy określić częstotliwość wdrażania najnowszych aktualizacji w systemach.

AXIS Camera Station Pro — zasady aktualizacji oprogramowania

W większości przypadków korzystanie z najnowszych wersji oprogramowania AXIS Camera Station Pro zapewnia dostęp do najnowszych poprawek zabezpieczeń neutralizujących wszystkie nowo odkryte luki. Dłuższe pozostawianie systemu bez poprawek zwiększa ryzyko wykorzystania tych luk przez intruzów i ewentualnego naruszenia bezpieczeństwa systemu.

Zalecane zasady i procedury
Ważne jest, aby sformułować zasady wprowadzania poprawek wraz z regularnymi ocenami wdrożonych wersji oprogramowania AXIS Camera Station Pro, które dadzą pewność, że jest ono aktualne. Zasady wprowadzania poprawek powinny również określać, kto odpowiada za zarządzanie czynnościami związanymi z aktualizowaniem zarówno oprogramowania serwerowego, jak i klienckiego. W przypadku oprogramowania AXIS Camera Station Pro najnowszą wersję można znaleźć na stronie *www.axis.com*. AXIS Camera Station Pro wymaga najnowszych bibliotek .NET, dlatego należy zadbać o zharmonizowanie zasad wdrażania poprawek systemu Windows z zasadami dotyczącymi oprogramowania AXIS Camera Station Pro.

Zasady aktualizacji oprogramowania sprzętowego urządzeń

Korzystanie z urządzeń z aktualnymi wersjami oprogramowania sprzętowego ogranicza większość typowych zagrożeń, ponieważ najnowsze wersje oprogramowania sprzętowego zawierają poprawki znanych luk w zabezpieczeniach, które intruzi mogą starać się wykorzystać. Axis udostępnia w ramach wsparcia długoterminowego specjalną wersję oprogramowania sprzętowego urządzeń, która zawiera ulepszenia zabezpieczeń i poprawki błędów, ale z ograniczonym zakresem dodatkowych funkcji, aby zapewnić długoterminową stabilność platformy. Więcej informacji na temat strategii Axis w zakresie rozwoju oprogramowania sprzętowego można znaleźć w dokumencie *Zarządzanie oprogramowaniem sprzętowym Axis*.

Zalecane zasady i procedury
W przypadku urządzeń zasady powinny określać wymóg aktualizowania całego oprogramowania sprzętowego. W konkretnych procesach można wykorzystać wbudowaną funkcję aktualizacji oprogramowania sprzętowego dostępną w oprogramowaniu AXIS Camera Station Pro lub narzędzie AXIS Device Manager Extend, za pomocą których można sprawdzać, czy są dostępne nowe wersje oprogramowania sprzętowego do urządzeń Axis. Należy zaplanować konkretną godzinę, najlepiej poza godzinami pracy, o której będą wdrażane wszystkie aktualizacje oprogramowania sprzętowego dla wszystkich kamer. AXIS Camera Station Pro / AXIS Device Manager Extend może również sprawdzać, czy aktualizacje oprogramowania sprzętowego zostały zaakceptowane. Jeśli system zawiera określone integracje, na które może wpłynąć aktualizacja, warto rozważyć standaryzację na bazie oprogramowania sprzętowego ze ścieżki wsparcia długoterminowego.

Bezpieczeństwo sieci

Zasady dostępu zdalnego

Urządzenia i usługi mające styczność z Internetem zwiększają ryzyko sondowania i wykorzystywania znanych luk w zabezpieczeniach przez intruzów z zewnątrz. Kamery mające styczność z Internetem, na przykład w niewielkich organizacjach potrzebujących zdalnego dostępu do materiału wideo, stają się łatwymi ofiarami, jeśli w organizacji używane są słabe hasła lub dojdzie do wykrycia nowej krytycznej luki w zabezpieczeniach. Zdalny dostęp do środowiska Windows powinien podlegać ścisłej kontroli, a w miarę możliwości należy go w ogóle unikać. O ile środowisko Windows może mieć łączność z Internetem do celów wygodnego aktualizowania systemów, korzystanie z usług pulpitu zdalnego, takich jak Windows Remote Desktop, TeamViewer czy AnyDesk, otwiera ścieżkę dostępu do systemu, jeśli usługi te nie są prawidłowo zarządzane.

Zalecane zasady i procedury
Należy bezwzględnie unikać ekspozycji adresu IP / portu kamery w sposób umożliwiający bezpośredni dostęp do niego z Internetu. Jeśli jest wymagany zdalny dostęp do materiału wideo, należy używać aplikacji Axis Secure Remote Access. AXIS Camera Station Pro wykorzystuje serwer dostępu zdalnego oparty na chmurze, aby ułatwić szyfrowany zdalny dostęp do systemu za pośrednictwem klienta AXIS Camera Station Pro lub aplikacji mobilnej AXIS Camera Station. Oprócz zarządzania połączeniami użytkowników zdalnych i mobilnych serwer dostępu zdalnego odgrywa ważną rolę w ochronie integralności, gdy z systemu korzystają użytkownicy zdalni. Więcej informacji na temat aplikacji Axis Secure Remote Access można znaleźć *tutaj*. Axis udostępnia pod swoją marką oficjalne aplikacje mobilne dla systemów Android i Apple iOS. Aplikację mobilną AXIS Camera Station należy pobierać wyłącznie z oficjalnych źródeł, czyli odpowiednio ze sklepów Google Play Store i Apple App Store.

Jeśli chodzi o dostęp przy użyciu pulpitu zdalnego do środowiska Windows, nie zaleca się umożliwiania tego rodzaju dostępu do systemu z oprogramowaniem AXIS Camera Station Pro. Jeśli jednak wystąpi taka konieczność, należy zachować szczególną ostrożność, aby zyskać pewność, że wybrana aplikacja pulpitu zdalnego jest bezpieczna, a dostęp do środowiska mają tylko osoby, które go rzeczywiście wymagają. Zachęcamy do wdrożenia dodatkowych warstw kontroli, takich jak uwierzytelnianie wieloskładnikowe (MFA). Stanowczo zaleca się rejestrowanie i późniejsze sprawdzanie prób połączeń zdalnych, ponieważ pozwala to ustalić, kto i w jakich porach uzyskuje zdalny dostęp do środowiska Windows.

Zasady ekspozycji sieci lokalnej

Zmniejszenie ekspozycji sieci lokalnej może pomóc w złagodzeniu wielu typowych zagrożeń przez ograniczenie powierzchni ataku. Istnieje wiele sposobów na zmniejszenie ekspozycji sieci, w tym fizyczna segmentacja sieci (oddzielny sprzęt i okablowanie sieciowe) oraz segmentacja logiczna przy użyciu wirtualnych sieci LAN (VLAN) i filtrowania adresów IP. Kamery Axis obsługują filtrowanie adresów IP (tabele adresów), dzięki czemu urządzenie odpowiada tylko na żądania połączeń pochodzące z dozwolonych, wprost wymienionych adresów IP.

Zalecane zasady i procedury
Rejestratory sieciowe AXIS Camera Station S22 to serwery sprzętowe z dwoma portami sieciowymi. Jeden z portów tworzy odseparowaną sieć dla kamer, a drugi łączy się z siecią (domeną) podstawową w celu obsługi klientów wideo. Serwer działa jako most i zapora dla sieci kamer, uniemożliwiając klientom bezpośredni dostęp do kamer. Zmniejsza to prawdopodobieństwo zagrożeń ze strony intruzów w sieci podstawowej.

Jeśli serwer AXIS Camera Station Pro i kamery są umieszczone w sieci podstawowej, zaleca się skonfigurowanie filtru IP kamer w taki sposób, aby ograniczyć dostęp tylko do serwerów obsługujących oprogramowanie AXIS Camera Station Pro, narzędzia AXIS Device Manager i dodatkowych klientów o charakterze konserwacyjnym.

Zasady szyfrowania sieciowego

Ruch sieciowy przesyłany za pośrednictwem niezabezpieczonych sieci zawsze powinien być szyfrowany. Internet zalicza się do sieci niezabezpieczonych. Również sieć lokalna może zostać sklasyfikowana jako niezabezpieczona, a wówczas przechodzący przez nią ruch także powinien być szyfrowany. Konkretna treść zasad stosowanych do ruchu wideo w sieci zależy od klasy materiału wideo i od ryzyka uzyskania przez intruzów dostępu do systemu wizyjnego za pośrednictwem sieci. Najlepiej jest założyć, że zabezpieczenia sieci już zostały naruszone. Większe organizacje zazwyczaj mają zasady określające sposób klasyfikowania sieci.

Zalecane zasady i procedury

Ruch między klientem wideo a serwerem AXIS Camera Station Pro powinien być zaszyfrowany. Ruch między serwerem AXIS Camera Station Pro a kamerami powinien być zaszyfrowany w zależności od infrastruktury. Kamery Axis domyślnie zawierają certyfikat z podpisem własnym i mają włączony protokół HTTPS. Jeśli istnieje ryzyko spoofingu sieciowego, na przykład w postaci złośliwego komputera próbującego podszyć się pod kamerę, należy skorzystać z infrastruktury klucza prywatnego (PKI) z certyfikatami podpisanymi przez urząd certyfikacji. AXIS Camera Station Pro ma wbudowany lokalny urząd certyfikacji, który umożliwia ekonomiczne zarządzanie podpisywaniem i dystrybucją certyfikatów serwera na potrzeby urządzeń Axis.

Wersje protokołu TLS

Zalecamy wyłączenie wersji 1.1 i 1.0 protokołu TLS. Instalator oprogramowania AXIS Camera Station udostępnia pomoc na etapie instalacji lub aktualizacji.

Szyfry HTTPS

AXIS Camera Station Pro obsługuje i wykorzystuje zestawy szyfrów TLS do bezpiecznego szyfrowania połączeń HTTPS. Konkretny zestaw szyfrów zależy od klienta, który łączy się z oprogramowaniem AXIS Camera Station Pro lub usługi będącej przedmiotem kontaktu, a AXIS Camera Station Pro negocjuje go zgodnie z protokołem TLS. Zalecamy skonfigurowanie systemu Windows w taki sposób, aby nie korzystał z zestawów szyfrów TLS 1.2 wymienionych *w dokumencie RFC 7540*. Możliwość wyłączenia zestawu szyfrów zależy od urządzeń i kamer używanych z oprogramowaniem AXIS Camera Station Pro. Jeśli urządzenie lub kamera wymaga określonego zestawu szyfrów, wyłączenie słabego zestawu szyfrów może nie być możliwe.

Zarządzanie danymi

Instalacja

AXIS Camera Station Pro umożliwia instalację w folderze nienależącym do standardowego katalogu plików programów. Może to jednak skutkować mniej rygorystyczną kontrolą dostępu, co stanowi potencjalne zagrożenie bezpieczeństwa. Zalecamy użycie domyślnej ścieżki instalacji lub zweryfikowanie uprawnień dostępu do wybranego folderu.

Uwaga

Jeśli ma zostać zmieniona lokalizacja kopii zapasowych bazy danych, należy użyć zabezpieczonej lokalizacji o ograniczonym dostępie. Udział sieciowy o powszechnym dostępie jest mniej bezpieczny.

Zasady bezpieczeństwa systemu

Klasyfikacja materiału wideo

Przekazywany na żywo i zarejestrowany materiał wideo należy poddać klasyfikacji. Materiał wideo można sklasyfikować jako publiczny, prywatny, o ograniczonym dostępie lub innego rodzaju stosownie do klas zdefiniowanych w zasadach organizacji. W wielu przypadkach materiał wideo podlega regulacjom prawnym i przepisom lokalnym, a także wewnętrznym zasadom IT, dlatego obowiązkiem właściciela systemu jest znajomość przepisów i regulacji mających zastosowanie do podlegających mu danych wideo.

Zalecane zasady i procedury
Materiał wideo przekazywany na żywo, zarejestrowany materiał wideo i materiał audio należy sklasyfikować zgodnie z organizacyjnymi zasadami klasyfikacji danych. Uprawnienia dostępu użytkowników i zabezpieczenia systemu należy skonfigurować odpowiednio do wrażliwości danych wideo i audio. Jeśli audio nie jest wymagane, można je wyłączyć na poziomie urządzenia.

Dodatkowe mechanizmy kontroli bezpieczeństwa

W zależności od poziomu dojrzałości organizacji i jej tolerancji ryzyka można wdrożyć kilka dodatkowych mechanizmów kontroli bezpieczeństwa określonych w dokumencie CIS Controls v8, aby ograniczyć zagrożenia cyberbezpieczeństwa występujące w codziennym funkcjonowaniu.

Dodatkowe mechanizmy kontrolne CIS:

Mechanizm 8: Zarządzanie dziennikami audytów
Zbieranie, przeglądanie i przechowywanie dzienników audytu zdarzeń, które mogą pomóc w detekcji ataków, poznawaniu ich przyczyn i usuwaniu ich skutków.

Mechanizm 14: Wdrożenie programu szkoleń i zwiększania świadomości w zakresie bezpieczeństwa
Poznawanie umiejętności i zachowań pracowników. Szkolenie pracowników w zakresie identyfikowania różnych form ataków.

Mechanizm 17: Reagowanie na incydenty i zarządzanie nimi
Korzystanie z pisemnych planów reagowania na incydenty z jasno określonymi fazami obsługi/zarządzania incydentami i rolami pracowników, a także sposobami zgłaszania incydentów bezpieczeństwa odpowiednim organom władz i stronom trzecim.

Przewodnik zabezpieczania systemów
AXIS Camera Station Pro

Wer. M2.3
Data: Listopad 2024
Nr katalogowy T10203603